CHECK POINT
5400 NEXT GENERATION SECURITY GATEWAY FOR THE SMALL ENTERPRISE

CHECK POINT 5400 NEXT GENERATION SECURITY GATEWAY

Small enterprise security

Product Benefits

- High performance protection against the most advanced cyber attacks
- Unique "first time prevention" for the most sophisticated zero day attack
- Optimized for inspecting SSL encrypted traffic
- Future-proofed technology safeguards against tomorrow's risks
- Centralized control and LOM improves serviceability
- Modular, expandable chassis with flexible I/O options

Product Features

- Simple deployment and management
- Secure remote access to corporate resources from a wide variety of devices
- One network expansion slot to add port density, fiber and fail-open IO card options
- Redundant appliance clustering technologies eliminate a single point of failure

OVERVIEW

The Check Point 5400 Next Generation Security Gateway combines the most comprehensive security protections to safeguard your small enterprise. The 5400 is a 1U Next Generation Security Gateway with one I/O expansion slot for higher port capacity, a 500GB (HDD) or 240GB (SSD) disk, and Lights-Out Management (LOM) for remote management. This powerful Next Generation Security Gateway is optimized to deliver real-world threat prevention to secure your critical assets and environments.

COMPREHENSIVE THREAT PREVENTION

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats require a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention with award-winning SandBlast™ Threat Emulation and Threat Extraction for complete protection against the most sophisticated threats and zero-day vulnerabilities.

Unlike traditional solutions that are subject to evasion techniques, introduce unacceptable delays, or let potential threats through while evaluating files, Check Point SandBlast stops more malware from entering your network. With our solution your employees can work safely no matter where they are and doesn't compromise their productivity.

PERFORMANCE HIGHLIGHTS

Firewall	IPS	NGFW[1]	Threat Prevention[2]
22 Gbps	3.9 Gbps	3.4 Gbps	1.745 Gbps

Performance measured under ideal testing conditions. Additional performance details on page 4.

1. Includes Firewall, Application Control, and IPS Software Blades.

2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades using R80.10.

ALL-INCLUSIVE SECURITY SOLUTIONS

Check Point 5400 Next Generation Security Gateways offer a complete and consolidated security solution available in two complete packages:

- NGTP: prevent sophisticated cyber-threats with Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and Email Security.
- NGTX: NGTP with SandBlast Zero-Day Protection, which includes Threat Emulation and Threat Extraction.

PREVENT KNOWN AND ZERO-DAY THREATS

The 5400 Next Generation Security Gateway protects organizations from both known and unknown threats with Antivirus, Anti-Bot, SandBlast Threat Emulation (sandboxing), and SandBlast Threat Extraction technologies.

As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

Furthermore, SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.

	NGTP	NGTX (SandBlast)
	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	✗	✓
SandBlast Threat Extraction	✗	✓

INSPECT ENCRYPTED CONNECTIONS

There is a shift towards more use of HTTPS, SSL and TLS encryption to increase Internet security. At the same time files delivered into the organization over SSL and TLS represent a stealthy attack vector that bypasses traditional security implementations. Check Point Threat Prevention looks inside encrypted SSL and TLS tunnels to detect threats, ensuring users remain in compliance with company policies while surfing the Internet and using corporate data.

INCLUSIVE HIGH PERFORMANCE PACKAGE

Customers with high connection capacity requirements can purchase the affordable High Performance Package (HPP). This includes the base system plus one 4x 1Gb SFP interface card, transceivers, Lights-Out-Management (LOM) and 16 GB of memory for high connection capacity.

	Base	HPP	Max
1 GbE ports (Copper)	10	10	18
1 GbE ports (Fiber)	0	4	4
Transceivers (SR)	0	4	4
RAM	8GB	16GB	32GB
AC or DC Power Units	1	1	1
Lights Out Management	Optional	Included	Included

REMOTE MANAGEMENT AND MONITORING

An optional Lights-Out-Management (LOM) card provides out-of-band remote management to remotely diagnose, start, restart and manage the appliance from a remote location. Administrators can also use the LOM web interface to remotely install an OS image from an ISO file.

SECURE REMOTE ACCESS

Each Check Point Next Generation Security Gateway is configured with mobile access connectivity for up to 5 users, using the Mobile Access Blade. This license provides secure remote access to corporate resources from a wide variety of devices including smartphones, tablets, PCs, Mac and Linux.

INTEGRATED SECURITY MANAGEMENT

Every Check Point appliance can either be managed locally with the available integrated security management[1] or via central unified management. Using local management, the appliance can manage itself and one adjacent appliance for high availability deployments.

[1] not available when purchased with the SSD option

5400 SECURITY GATEWAY

1. Sync 10/100/1000Base-T RJ45 port
2. RJ45/micro USB console port
3. One network card expansion slot
4. 8x 10/100/1000Base-T RJ45 ports
5. Management 10/100/1000Base-T RJ45 port
6. 2x USB ports for ISO installation
7. Lights-Out Management port
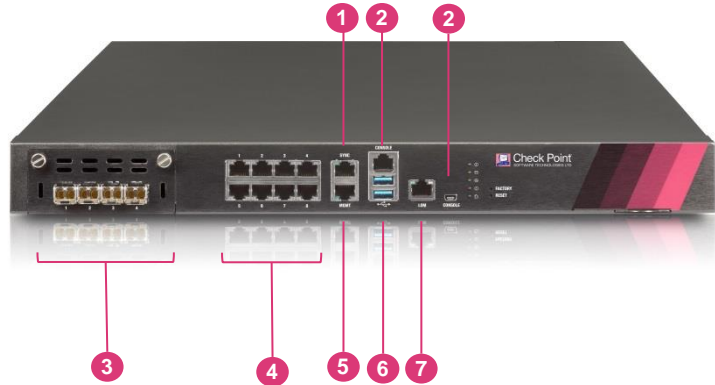
ORDERING INFORMATION

BASE CONFIGURATION [1]	
5400 Next Generation Security Gateway Base Configuration, includes 10x1GbE copper ports, 8GB RAM, 1 HDD, 1 AC Power Unit, Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year.	CPAP-SG5400-NGTP
5400 SandBlast Next Generation Security Gateway Base Configuration, includes 10x1GbE copper ports, 8GB RAM, 1 HDD, 1 AC Power Unit, SandBlast (NGTX) Security Subscription Package for 1 Year	CPAP-SG5400-NGTX

HIGH PERFORMANCE PACKAGES [1]	
5400 Next Generation Security Gateway with High Performance Package, includes10x1GbE copper ports, 4x1Gb SFP ports, 4 SR transceivers, 16 GB RAM, 1 HDD, 1 AC Power Unit, Lights Out Management (LOM), Next Generation Threat Prevention (NGTP) Security Subscription Package for 1 Year	CPAP-SG5400-NGTP-HPP
5400 Next Generation Security Gateway with High Performance Package, includes10x1GbE copper ports, 4x1Gb SFP ports, 4 SR transceivers, 16 GB RAM, 1 HDD, 1 AC Power Unit, Lights Out Management (LOM), Next Generation Threat Extraction (SandBlast) Security Subscription Package for 1 Year	CPAP-SG5400-NGTX-HPP

[1] SKUs for 2 and 3 years, for High Availability and Appliances with an SSD or DC power option are also available, see the online Product Catalog

ACCESSORIES

INTERFACE CARDS AND TRANSCEIVERS	
8 Port 10/100/1000 Base-T RJ45 interface card	CPAC-8-1C-B
4 Port 1000Base-F SFP interface card; requires additional 1000Base SFP transceivers	CPAC-4-1F-B
SFP transceiver module for 1G fiber ports - long range (1000Base-LX)	CPAC-TR-1LX-B
SFP transceiver module for 1G fiber ports - short range (1000Base-SX)	CPAC-TR-1SX-B
SFP transceiver to 1000 Base-T RJ45 (Copper)	CPAC-TR-1T-B
4 Port 1GE copper Bypass (Fail-Open) network interface card (10/100/1000 Base-T)	CPAC-4-1C-BP-B

SPARES AND MISCELLANEOUS	
Memory upgrade kit from 8GB to 16GB for 5400 appliance	CPAC-RAM8GB-5000
Memory upgrade kit from 8GB to 32GB for 5400 appliance	CPAC-RAM24GB-5000
Memory upgrade kit from 16GB to 32GB for 5400 appliance	CPAC-RAM16GB-5000
Lights Out Management module	CPAC-LOM-B
Slide rails for 5000 Appliances (22" - 32")	CPAC-RAIL-5000
Extended slide rails for 5000 Appliances (24" - 36")	CPAC-RAIL-EXT-5000

Performance

Ideal Testing Conditions

- 22 Gbps of UDP 1518 byte packet firewall throughput
- 3.9 Gbps IPS
- 3.4 Gbps of NGFW[1]
- 1.745 Gbps of Threat Prevention[2]
- 2.16 Gbps of AES-128 VPN throughput
- 150,000 connections per second, 64 byte response
- 3.2/6.4/12.8 million concurrent connections, 64 byte response[3]

Real-World Production Conditions

- 600 SecurityPower Units
- 10 Gbps of firewall throughput
- 1.08 Gbps IPS
- 690 Mbps of NGFW[1]
- 395 Mbps of Threat Prevention[2]

Virtual Systems

- Maximum VS (base/HPP/max memory): 10/20/20

Your performance may vary depending on different factors. Visit www.checkpoint.com/partnerlocator to find an appliance that matches your unique requirements.

1. Includes Firewall, Application Control and IPS Software Blades. 2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades using R80.10. 3. Performance measured with default/HPP/maximum memory.

Expansion Options

Base Configuration

- 10 on-board 10/100/1000Base-T RJ-45 ports
- 1x CPUs, 2x physical cores, 2x virtual cores (total)
- 8 GB memory (16 and 32 GB options)
- 1x 500GB (HDD) or 1x 240GB (SSD) drive
- 1 power supply (AC or DC)
- Fixed rails (slide rail option)
- (Lights-Out-Management (LOM) option)

Network Expansion Slot Options (1 slot available)

- 8x 10/100/1000Base-T RJ45 port card, up to 18 ports
- 4x 1000Base-F SFP port card, up to 4 ports

Fail-Open/Bypass Network Options

- 4x 10/100/1000Base-T RJ45 port card

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active and Active/Passive - L3 mode
- Session failover for routing change, device and link failure
- ClusterXL or VRRP

IPv6

- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

Unicast and Multicast Routing (see SK98226)

- OSPFv2 and v3, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3

Physical

Power Requirements

- Single Power Supply Rating: 250W
- AC power input: 110-240V (47-63Hz)
- Power consumption maximum: 76.5W
- Maximum thermal output: 261 BTU/hr.

Dimensions

- Enclosure: 1RU
- Dimensions (W x D x H): 17.2x16x1.73 in. (438x406.5x44mm)
- Weight: 14 lbs. (6.37 kg)

Environmental Conditions

- Operating: 0° to 40°C, humidity 5% to 95%
- Storage: –20° to 70°C, humidity 5% to 95% at 60°C

Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, WEEE, REACH[1], ISO14001[1]

[1] factory certificate